Adrian R. Bacon, Esq. (SBN 280332)
LAW OFFICES OF TODD M. FRIEDMAN
21031 Ventura Blvd, Suite 340
Woodland Hills, CA 91364
Tel.: (323) 306-4234
Facsimile: (866) 633-0228
Email: abacon@toddflaw.com

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

ANDREW ROSE, JEREMY LEBMAN and PATRICIA HERVEY on Behalf of Themselves and All Others Similarly Situated,

Plaintiffs,

v.

SANSUM CLINIC and META PLATFORMS, INC.,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Andrew Rose, Jeremy Lebman, and Patricia Hervey ("Plaintiffs"), individually on behalf of themselves and all others similarly situated, by and through their undersigned counsel, bring this Class Action Complaint against Defendants Sansum Clinic ("Healthcare Defendant" or "Sansum") and Meta Platforms, Inc. ("Facebook") (collectively "Defendants"). The allegations in this Complaint are based upon the personal knowledge of Plaintiffs, and on information and belief as to all other matters through investigation of Plaintiffs' counsel.

NATURE OF THE ACTION

1. This putative class action is brought on behalf of all persons, users, prospective patients, and current patients who visited the Healthcare Defendant's website https://www.sansumclinic.org/ (hereinafter, the "Website"), utilized the Website for its various intended purposes, and had their private health conditions, identities, actual or potential medical

treatments, and the hospitals they visited or may visit disclosed to Facebook without their knowledge or consent (hereinafter, "PII User").

2. Plaintiffs and the Class Members seek damages associated with Healthcare Defendant's violation of their privacy rights under the California Information Protection Act ("CIPA") Cal. Penal Code §§ 630, *et seq*.; Federal Wiretap Act 18 U.S.C. § 2510, *et. seq*. (the "Wiretap Act"); California Confidentiality of Medical Information Act ("CMIA"); and common law claims for invasion of privacy, breach of contract, negligence, and intrusion upon seclusion.

3. Healthcare Defendant's "Website Privacy Notice" informs PII Users that "[Sansum is] aware of the need for complete confidentiality and [is] dedicated to protecting your personal information and safeguarding your individual privacy whenever you are accessing the website to partake or simply to search."[1] Throughout Healthcare Defendant's privacy notice, Sansum emphasizes the importance of keeping PII Users' confidential personal health information safe from unauthorized disclosure. The Notice of Privacy Practices also describes how Healthcare Defendant may use and disclose information about PII Users to others outside Sansum, however, none of these notices indicate that Sansum will disclose private health information ("PHI") to Facebook for Facebook's own use and monetary gain.[2]

4. Since its creation in 2004, Facebook has evolved into a social media giant, which has allowed it to take advantage of its massive audience to become one of the largest advertising companies in the world.[3]

5. In order to optimize its advertising business, Facebook collects data regarding users' interactions with websites across the internet. One of the ways Facebook collects this user data is through the use of the "Facebook Pixel" (hereinafter the "Pixel").

6. The Pixel is a snippet of computer code that Healthcare Defendant places on its Website and when a user visits the Website, the Pixel allows Healthcare Defendant to collect the

[1] *Website Privacy Notice*, SANSUM CLINIC https://www.sansumclinic.org/privacy (last visited August 3, 2023).
[2] *Id*.
[3] *Facebook Ad Revenue (2017-2026)*, OBERLO https://www.oberlo.com/statistics/facebook-ad-revenue (last visited August 3, 2023).

PHI of its users and share it with Facebook.[4] Specifically, Healthcare Defendant tracks users' activities on the Website by utilizing the Pixel, which intercepts the PHI of PII Users, such as the search terms used by a PII User on the Website, what health condition the user is searching for, the specific doctors that PII Users searches for and their area of expertise, and other information related to the PII User's use of the Website, along with the user's Facebook ID (FID). The users' PHI and FID are packaged together and then sent via a single data transmission to Facebook, enabling Facebook to identify users and associate users' profiles to users' PHI. This occurs even when the PII User has not consented or authorized the Healthcare Defendant to share such information, pursuant to the CMIA and other statutes.

7. The Website was coded to include the Pixel, which Healthcare Defendant has allowed to operate on its website, and which results in Healthcare Defendant's sharing of users' PHI with Facebook. The Pixel monitors for events specified by the Healthcare Defendant and sends users' FID and PHI to Facebook whenever that Pixel Event occurs on the Website ("Pixel Events"). In this case, Healthcare Defendant's data sharing is automatically triggered when a PII User visits any of Healthcare Defendant's webpages with a PageView and/or Microdata Pixel Event active on Healthcare Defendant's webpages. As detailed more fully below, these Pixel Events trigger when a PII User conducts searches on the Website, including for information or services relating to a specific health condition. When a user performs these actions, and has previously or is currently signed into Facebook using the same browser used to access the Website, the Website triggers one or more of the Pixel Events and the user's PHI is automatically shared with Facebook. Accordingly, the Pixel allows Facebook to know the health conditions of the PII Users of the Website, the location and type of doctor(s) users searched for, and what type of health information users searched for on the Website. Additionally, as the search results on the Website include services offered by Healthcare Defendant related to what was searched, the Healthcare Defendant utilizes PII User's information to recruit PII Users to use their services.

[4] *Meta for Developers: Meta Pixel*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/ (last visited August 3, 2023).

8. Defendant shares the PII—i.e., the users' unique FID and PHI—as one data point to Facebook. Because the user's FID uniquely identifies an individual's Facebook user account, Facebook—or any other ordinary person—can use it to quickly and easily identify the account holder and view that user's corresponding Facebook profile.

9. The Website's PII Users are not adequately informed about the dissemination of their PHI. PII Users are not given an opportunity to consent to the dissemination of their PHI; instead, it is automatic. PII Users cannot exercise reasonable judgment to defend themselves against the methods used by Healthcare Defendant to collect and use their PHI.

10. Incorporation of the Pixel onto the Website provides numerous benefits to Healthcare Defendant. One such benefit is allowing Healthcare Defendant to analyze user experiences and behavior on the Website to assess the Website's traffic and functionality. Use of the Pixel also allows Healthcare Defendant to target or retarget their PII Users with advertisements, along with measuring how well those advertisements are working.

11. Facebook also benefits directly when a third-party website implements the Pixel. When placed on a third-party website, the Pixel allows Facebook to surreptitiously gather information regarding all user interactions with the website. Facebook then aggregates the data it collects across all the websites that implement the Pixel.[5] By collecting this user information, Facebook can improve its machine-learning algorithm to better identify and target users across the web, improving the effectiveness of its advertising services, ultimately making Facebook more marketable as an advertising broker.

12. The described data collection methods make the Pixel's integration into healthcare websites, which serve as repositories for confidential medical data, all the more concerning.

13. As alleged more fully below, when a PII User of the Healthcare Defendant's Website inputs information into the Website to search for symptoms related to a health condition, that information is transmitted to Facebook through the Pixel. Depending on the search, this

[5] *Business Help Center: About Facebook Pixel*, FACEBOOK https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited on August 3, 2023); and *Business Center Help: Metrics and estimates using Accounts Center accounts*, FACEBOOK https://www.facebook.com/business/help/283579896000936 (last visited on August 3, 2023).

information may include explicit details regarding that PII User's potential or actual medical conditions, along with symptoms they may be experiencing.

14. The information transmitted through the Pixel includes health conditions (e.g., cancer or pregnancy), medications, allergies, and other forms of PHI, which is then used by Facebook to better target users with advertisements.

15. Healthcare Defendant's tracking, sharing, interception, and storage of information – directly, and as aider and abettor to Facebook's interception – violates Plaintiffs' and Class Members' statutorily-protected privacy in their protected health information, including their current or potential medical conditions, the effect those medical conditions have on their lives, the symptoms of those medical conditions, and health concerns that users may be experiencing, tied to their personally identifiable information.

16. Through the enactment of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and regulations codified by the United States Department of Health and Services ("HHS"), national standards were established to protect the confidential health information of patients across the United States. [6]

17. By visiting the Website, Plaintiffs and Class Members entrusted Healthcare Defendant with their PII and PHI. Plaintiffs and Class Members had a reasonable expectation that their PHI and PII would be kept safe from unauthorized disclosure.

18. In violation of that trust, and in contravention of their own privacy terms, Healthcare Defendant disclosed Plaintiffs' and Class Members' private health information to Facebook without authorization or consent to further Healthcare Defendant's own commercial interests. Healthcare Defendant has thus failed to safeguard Plaintiffs' and Class Members' sensitive personal, including health, information in violation of federal and state law.

---

[6] HIPPA defines personal health information as individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records. "Individually identifiable health information" is information, including demographic data, that relates to: (1)the individual's past, present or future physical or mental health or condition, (2) the provision of health care to the individual, or (3) the past, present, or future payment for the provision of health care to the individual; and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

19. Defendants have each profited from these unauthorized disclosures of Plaintiffs' and Class Member's PHI as explained below. The collection of such data additionally allowed pharmaceutical and other related companies to send targeted advertising to Plaintiffs and Class Members based on their PHI.

20. Without Facebook's unlawful data collection, Plaintiffs would not have been subjected to personalized advertisements based on their PHI, including advertisements shown based on the sensitive PHI users provided to the Website.

21. As part of Facebook's advertising operations, Facebook customizes and directs these advertisements specifically toward Plaintiffs and Class Members. Facebook offers, sells, and profits from the access it provides third parties to individuals who are highly likely to be interested in their products or services, commonly referred to as a target audience.

22. Despite Facebook's knowledge that the Pixel collects highly sensitive PHI on the Website, Facebook continues to collect and profit from the information collected.

23. Moreover, Healthcare Defendant knew or had reason to know that by implementing the Pixel on its Website, it would cause the collection and sharing of Plaintiffs' and Class Members' sensitive PHI.[7]

24. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs and Class Members seek relief in this action individually and on behalf of users of the Website for violations of their right to privacy and for violations of various federal and state laws.

THE PARTIES

A. Plaintiffs

25. Plaintiff Andrew Rose is a resident of Ventura, California. In or around 2021, began visiting the Website. Plaintiff Rose has a Facebook account and has been a user of Facebook since around 2005. Plaintiff Rose has used the Website to search for information related to health conditions or suspected health conditions on a computer or other device, for both himself, and his

[7] *Meta Business Tools Terms*, FACEBOOK https://www.facebook.com/legal/businesstech (advising Pixel users, like the Healthcare Defendant, of the tracking tool's capabilities) (last visited August 3, 2023).

family members. Specifically, Plaintiff Rose's use of the Website included using the Website's search function in a Chrome web browser to search for information related to symptoms he was experiencing within the past six (6) months. Plaintiff Rose's Facebook profile contains information like his name, occupation, place of residence, and other personal information. While utilizing the Website, Plaintiff Rose was signed into his Facebook profile, or had signed into his Facebook profile in the same browser within the past year.

26. Plaintiff Jeremy Lebman is a resident of North Hollywood, California. In or around 2021, Plaintiff Lebman began visiting the Website. Plaintiff Lebman has a Facebook account and has been a user of Facebook since approximately 2009. Plaintiff Lebman has used the Website to search for information related to health conditions and suspected health conditions as recently as 6 months ago. Plaintiff Lebman's Facebook profile contains personal information such as his name, occupation, place of residence, and other personal information. While utilizing the Website, Plaintiff Lebman was signed into his Facebook profile, or had signed into his Facebook profile in the same browser within the past year.

27. Plaintiff Patricia Hervey is a resident of Lake Forest, California. In or around 2021, Plaintiff Hervey began visiting the Website. Plaintiff Hervey has a Facebook account and has been a user of Facebook since approximately 2017. Plaintiff Hervey has used the Website to search for information related to health conditions or suspected health conditions, and to search for doctors and services to treat actual or potential medical conditions. Specifically, Plaintiff Hervey's use of the Website included using the Website's search function in various browsers to search for information related to a condition and potential procedures as recently as three (3) months ago. Plaintiff Hervey's Facebook profile contains personal information such as her name, occupation, place of residence, and other personal information. While utilizing the Website, Plaintiff Hervey was signed into her Facebook profile, or had signed into her Facebook profile in the same browser within the past year.

B. Defendants

28. Defendant Sansum Clinic is a non-profit health system company with headquarters at 470 South Patterson Ave., Santa Barbara, CA 93111. Sansum encourages its thousands of PII

Users and prospective PII Users to utilize the Website to search for information related to their health conditions and search for hospital locations and doctors.

29. Defendant Meta Platforms, Inc. (f/k/a Facebook, Inc.) is a Delaware corporation and multinational technology company with its principal place of business at 1 Hacker Way, Menlo Park, California.

JURISDICTION AND VENUE

30. This Court also has jurisdiction under 28 U.S.C. § 1332(d) because this action is a class action in which the aggregate amount in controversy for the proposed Class (defined below) exceeds $5,000,000, and at least one member of the Class is a citizen of a state different from that of either Defendant.

31. This Court has personal jurisdiction because Defendants' principal places of business are in California, and they derive revenue in the State of California.

32. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants do business in and are subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

COMMON FACTUAL ALLEGATIONS

A. Legislative Backgrounds

a. Background to the Federal Wiretap Act

33. The Federal Wiretap Act (the "Wiretap Act") was enacted in 1934 "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications."[8]

34. The Wiretap Act was primarily concerned with government's use of wiretaps but was amended in 1986 through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[9]

---

[8] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, WASHINGTON AND LEE JOURNAL OF CIVIL RIGHTS AND SOCIAL JUSTICE, https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj (last visited August 3, 2023).

[9] *Id.* at 192.

35. Congress was concerned that technological advancements were rendering the Wiretap Act out-of-date, such as "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing."[10]

36. As a result, the ECPA primarily focused on two types of computer services which were prominent in the 1980s: (i) electronic communications such as email between users; and (ii) remote computing services such as cloud storage or third-party processing of data and files.[11]

37. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

38. While communicating with Healthcare Defendant, users had the contents of their communications shared with Facebook.

b. Background to the California Invasion of Privacy Act

39. CIPA was enacted in 1967 for the expressly stated purpose "to protect the right of privacy of the people of [California]."[12] The California legislators were concerned about emergent technologies that allowed for the "eavesdropping upon private communications," believing such technologies "created a serious threat to the free exercise of personal liabilities and cannot be tolerated in a free and civilized society."[13]

40. CIPA is regularly recognized as California's analog to the Federal Wiretap Act, comprised of the same general elements and protect against the same general harms.

41. To protect people's privacy, legislators broadly protected wired and aural communications being sent to or received from California.[14] Notably, for wired communications, California set out to prohibit (i) intentional wiretapping or (ii) willful attempts to learn the contents of wired communications, (iii) attempts to use or transmit information obtained through

---

[10] Senate Rep. No. 99-541, at 2 (1986).
[11] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).
[12] Cal. Penal Code § 630.
[13] *Id.*
[14] Cal. Penal Code § 631-32.

wiretapping, or (vi) aiding, agreeing with, employing, or conspiring with any person(s) to unlawfully do, permit, or cause the preceding three wrongs.[15]

42. CIPA also prohibits the manufacture, assembly, sale, offer for sale, advertisement for sale, possession, or furnishment to another of devices which are primarily or exclusively designed or intended for eavesdropping upon the communication of another.[16]

c. Background on California Confidentiality of Medical Information Act

43. The CMIA is a California law that governs the privacy and security of medical information for residents of California. The CMIA is designed to protect the confidentiality of an individual's medical information and ensure that healthcare providers and similar entities handle such medical information with care and in a responsible manner. The CMIA was established to provide comprehensive regulations and protections for the privacy and confidentiality of medical information within the state of California. The CMIA applies to a wide range of healthcare providers, health plans, and other entities that handle medical information, including those handling the software for healthcare provider's websites. Cal. Civ. Code §§ 56.06 et al.

44. Through its enactment, the California legislature recognized the sensitive nature of medical information and the need to protect individual's privacy rights in the healthcare context. The legislature sought to provide clear standards to healthcare providers regarding how medical information of such providers can be handled. The CMIA sought also to provide guidance as how the proper dissemination of healthcare information in can be made, such as for treatment, payment, and healthcare operations.

B. How Websites (and the Internet) Operate

45. Websites are hosted on servers, but "run" on a user's internet browser.

46. Websites are a collection of webpages, and each webpage is essentially a document containing text written in HyperText Markup Language (HTML) code.[17]

---

[15] *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1134 (E.D. Cal. 2021) (citing *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978)).

[16] Cal. Penal Code § 635.

[17] *What is the difference between webpage, website, web server, and search engine?*, MOZILLA https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/Pages_sites_servers_and_search_engines (last visited August 3, 2023).

47. Webpages each have a unique address, and two webpages cannot be stored at the same address.[18]

48. When a user navigates to a webpage (such as entering a URL address directly or clicking a hyperlink containing the address), the browser contacts the DNS server, which translates the web address of that website into an IP address.[19]

49. An IP (Internet Protocol) address is "a unique address that identifies a device on the internet or a local network."[20] Essentially, an IP address is:

> the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

50. The user's browser then sends an HTTP Request to the server hosting that IP address, requesting a copy of the website be sent to the user, which, if approved, receives a HTTP Response that authorizes the HTTP Request and begins the process of sending the webpage's files to the user in small chunks.[21]

51. The user's browser then assembles the small chunks back into HTML, which is then processed by the user's browser and "rendered" into a visual display according to the instructions of the HTML code.[22] This is the visible, and usually interactable, website that most people think of.

C. Facebook's Advertising Business and Pixel

52. Facebook was founded in 2004 by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes. Facebook began as a social networking website for college

---

[18] *Id.*
[19] *How the web works*, MOZILLA https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited August 3, 2023).
[20] *What is an IP Address – Definition and Explanation*, KASPERSKY https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address (last visited August 3, 2023).
[21] *Id.*
[22] *Id.*

students,[23] and quickly saw success gaining more than one million users in 2004, and more than six million by 2005.

53. By 2008, Facebook's popularity surpassed Myspace, making it the leading social networking platform. [24]

54. Recognizing the significance of having direct connection to millions of consumers, Facebook initiated the monetization of its platform in 2007 through the introduction of "Facebook Ads."[25] This new advertising approach promoted a "completely new way of advertising online" that would enable advertisers to deliver more personalized and pertinent advertisements.[26]

55. At present, Facebook offers advertising services on its own platforms, including Facebook and Instagram, in addition to external websites through the Facebook Audience Network.[27] Facebook now has over 2.9 billion active users and has extensive advertising reach[28]

56. Facebook provides various advertising targeting options which cater to an advertiser's desired audience. These options include "Core Audiences," "Custom Audiences," "Look Alike Audiences,"[29] and a more detailed targeting approach known as "Detailed Targeting." Each of these advertising tools enables advertisers to focus on specific users based on their personal data, which includes factors such as geographic location, demographics, interests, connections, and behaviors among other criteria.[30] The creation of such audiences can be done by Facebook, the advertiser, or a combination of both.

57. Based on Facebook's ability to target specific users so precisely, it is unsurprising that Facebook's advertising service swiftly emerged as the most prosperous business division

---

[23] Jay Fuchs, *How Facebook Ads Have Evolved [+What This Means for Marketers]*, HUBSPOT (June 11, 2021), https://blog.hubspot.com/marketing/history-facebook-adtips-slideshare (last visited August 3, 2023).
[24] Michael Arrington, *Facebook No Longer The Second Largest Social Network*, TECHCRUNCH (June 13, 2008) https://techcrunch.com/2008/06/12/facebook-no-longer-the-second-largest-social-network/ (last visited on August 3, 2023).
[25] *Facebook Unveils Facebook Ads*, FACEBOOK (Nov. 6, 2007) https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/ (last visited August 3, 2023).
[26] *Id.*
[27] *Business Help Center: About Meta Audience Network*, FACEBOOK https://www.facebook.com/business/help/788333711222886?id=571563249872422 (last visited August 3, 2023).
[28] *Id.*
[29] *Target Audiences: Hitting The Bullseye With Facebook Ads*, SPRAGUE MEDIA https://spraguemedia.com/blog/target-audiences-bulleye-with-facebook-ads/ (last visited August 3, 2023).
[30] *Id.*

within Facebook. Millions of companies and individuals avail themselves of Facebook's advertising offerings.

58. In 2009, Meta generated $761 million in revenue through its advertising operations. A decade later, Facebook's advertising revenue skyrocketed, experiencing an exponential growth of almost 100 times.[31]

59. As shown below, Facebook generates essentially all of its revenue from selling advertising placements to marketers.

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$117.93 billion	$114.93 billion	97.46%
2020	$85.97 billion	$84.17 billion	97.90%
2019	$70.70 billion	$69.66 billion	98.52%
2018	$55.84 billion	$55.01 billion	98.51%
2017	$40.65 billion	$39.94 billion	98.25%

60. Indeed, their advertising revenues have continued to grow: a recent report indicates that Facebook's revenues from advertising alone are set to hit $153.76 billion in 2023, representing a 13.1% increase from 2022.[32]

61. Facebook's ad-targeting capabilities have faced consistent scrutiny due to its capacity to target individuals using highly detailed data. For example, Meta reached a settlement with the Department of Justice regarding its Lookalike Ad service in 2022. The Lookalike Ad service allowed discriminatory targeting by landlords based on race and other demographic factors, resulting in a violation of federal law.

D. Facebook's Pixel

62. According to Peter Eckersley, the Chief Computer Scientist at the Electronic Frontier Foundation, Facebook's tracking tools enable Facebook to gather extensive information about individuals, and with the help of artificial intelligence, analyze the behavior of those

[31] Rishi Iyengar, *Here's how big Facebook's ad business really is*, CNN BUSINESS (July 1, 2020), https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited August 3, 2023).
[32] *Facebook Ad Revenue (2017-2026)*, OBERLO https://www.oberlo.com/statistics/facebook-ad-revenue (last visited August 3, 2023).

individuals.[33] The comprehensive knowledge resulting from implementation of its tracking tools is ideal for advertising purposes, allowing for highly targeted and effective targeted advertising campaigns.

63. Facebook employs diverse tracking methods to gather data about individuals, which includes incorporating software development kits into third-party applications[34], utilizing "Like" and "Share" buttons (referred to as "social plug-ins"), and employing various other methodologies.[35] This accumulated data is subsequently leveraged to enhance Facebook's advertising business. One of the most notable tools in Facebook's tracking arsenal is the Pixel, which was introduced in 2015 and holds significant influence as described below.[36]

64. Facebook promotes the Pixel as an innovative solution for reporting and optimizing conversions (clicks to purchases), audience building, and gaining valuable insights into website usage. Facebook emphasized that website owners could easily utilize the Pixel by embedding an image that occupies a single pixel on a webpage, enabling them to track and optimize conversions. This feature allows website owners and advertisers to gauge the effectiveness of their advertising efforts by monitoring the actions taken by individuals on their website.

65. For Facebook, the Pixel serves as a channel for collecting and transmitting information collected by websites utilizing the Pixel to Facebook. This information is relayed through scripts on the website, executed within the user's internet browser.

66. Facebook also has the ability to connect the data with a user's Facebook account using the "Facebook Cookie." This cookie serves as a solution to counteract cookie-blocking

---

[33] Sam Harnett, *Here's the Data Facebook Has on Users and How the Company Gathers It*, KQED (Mar. 22, 2018) https://www.kqed.org/news/11657315/heres-the-data-facebook-has-on-users-and-how-the-company-gathers-it (last visited August 3, 2023).

[34] *How Facebook tracks you in Android (even if you don't have a Facebook account)*, MEDIUM (Nov. 11, 2019) https://medium.com/codomo/how-facebook-tracks-you-on-android-even-if-you-dont-have-a-facebook-account-92613e0c017a (last visited August 3, 2023).

[35] *Meta for Developers: Social Plugins*, FACEBOOK https://developers.facebook.com/docs/plugins/ (last visited August 3, 2023).

[36] Cecile Ho, *Announcing Facebook Pixel*, FACEBOOK (Oct. 14, 2015) https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/ (last visited August 3, 2023).

methods, including one created by Apple, Inc., that aim to monitor user activities.[37] Cookies, or small data files placed on a user's PC while using a website, are often used as a means to store information about a user's identity or activity on websites. While companies like Apple, Inc. try to limit cookie functionality, Facebook has developed a first-party cookie that serves as a solution to counteract cookie-blocking methods.[38]

67. A function of the Pixel is to gather, collect, and then share user information with Facebook.[39] This information enables Facebook and the web developers to build valuable personal profiles for users, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.[40]

68. The surreptitious communications described above happen without the users' knowledge.

69. Once installed, the Pixel provides website owners with data and analytics tools about ads which they have placed on Facebook and the various tools being used to target people who have visited their website. An article published by markup.org confirms this functionality.[41]

70. Web developers and website operators can choose to use the Pixel to share both user activity and user identity with Facebook.

71. The information collected by the Pixel is sent to Facebook with PII, which includes the user's IP address, name, email, phones number, and specific Facebook ID that points to the user's Facebook profile. This PII is stored across a number of cookies and by Facebook on its servers, which it maintains for years in some cases.[42]

72. Despite claiming to "hash" PII provided by PII User, Facebook actually utilizes the hashed format with the specific intention of linking Facebook Pixel data to Facebook profiles.

---

[37] *What Facebook's First-Party Cookie Means for AdTech*, CLEARCODE https://clearcode.cc/blog/facebook-first-party-cookie-adtech/ (last visited August 3, 2023).
[38] *Id.*
[39] Pixel allows websites to track visitor activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta for Developers: Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/ (last visited on August 3, 2023).
[40] *See Meta Pixel*, FACEBOOK, https://www.facebook.com/business/tools/meta-pixel (last visited on August 3, 2023).
[41] Todd Feathers, et al., *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (July 19, 2023) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited on August 3, 2023).
[42] *Id.*

Facebook has engineered the Pixel in a way that allows it to receive real-time information about PII User's actions on the medical provider's online platforms. Whenever a PII User performs any action on a webpage that includes Pixel, such as clicking buttons for registration, login, logout, or appointment creation on a PII User portal, the embedded Facebook code intercepts the content of the PII User's interaction to Facebook while the communication between the PII User and the medical provider is still ongoing.

73. Between the 33 top 100 hospitals that were discovered to have Pixel report on by the markup.org article, which similarly collect and transmit PII User appointment information to Facebook, these hospitals together reported over 26 million PII User admissions and visits in the year 2020 alone. The total number of affected PII Users will inevitably trend higher as The Markup's investigation was limited to slightly over 100 hospitals.

74. One legal officer at Privacy International, Laura Lazaro Cabrera, highlighted that even having access to a portion of these data points, such as solely the URLs accessed by users, poses concerns regarding Facebook's usage. In reasoning, Cabrera emphasized that users should: "'[t]hink about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data.'"[43]

75. In a recent development, employees at Facebook acknowledged the insufficient safeguards in place for protecting sensitive data. Engineers working on the ad and business product team at Facebook expressed in a privacy overview from 2021 that they lack the necessary level of control and transparency regarding the utilization of data within their systems during a privacy overview in 2021.[44]As a result, they are unable to make well-informed policy changes or external commitments, such as stating with confidence that they will not use specific data for certain purposes.

---

[43] Grace Oldham and Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients (last visited August 3, 2023).

[44] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document* (Apr. 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-orwhere-it-goes (last visited August 3, 2023).

76. Website owners – such as Defendant Sansum Clinic– hold the decision-making authority to add the Pixel code to its webpages. The owner may not hand-select every detail associated with the website, ranging from the use of certain font, colors, etc., to the employment of tracking tool, such as the Pixel, or a keystroking monitor, or which and whether terms and conditions should be associated with its website, newsletter, or any other aspect of its business. The level of management or oversight by the owner, however, does not alter or reduce, and certainly does not eliminate, its responsibility over the functionality of its website made available to visitors, or what is gathered about its user and then shared with third parties.

a. Defendants added the Pixel to the Website

77. To activate and employ a Facebook Pixel, a website owner must first sign up for a Facebook account, where specific "business manager" accounts are provided the most utility for using the Pixel.[45] For instance, business manager accounts can: (i) create and utilize more simultaneous Pixels, (ii) manage multiple Facebook Ad Accounts and Pages from a centralized interface, (iii) access and manage by multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees), (iv) build custom audiences for multiple ad campaigns, and (v) eliminate privacy concerns related to using a personal profile for business purposes.[46]

78. The website operator must utilize the tools made available to it by Facebook in order to cause the Pixel to be created and added to its site. The process begins with the website operators' naming of the Pixel at the time of its creation.[47]

79. Once the Pixel is created, the website operator will assign access to the Pixel to specific people for management purposes,[48] as well as connect the Pixel to a Facebook Ad account.[49]

---

[45] *Business Help Center: How to create a Meta Pixel in Business Manager*, FACEBOOK, https://www.facebook.com/business/help/314143995668266?id=1205376682832142 (last visited August 3, 2023).
[46] Jacqueline Zote, *A step-by-step guide on how to use Facebook Business Manager* (June 14, 2021), SPROUTSOCIAL https://sproutsocial.com/insights/facebook-business-manager/ (last visited August 3, 2023).
[47] *Id.; see also* Ivan Mana, *How to Set Up & Install the Facebook Pixel (In 2022)*, YOUTUBE https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited August 3, 2023).
[48] *Business Help Center: Add People to Your Meta Pixel in Your Meta Business Manager*, FACEBOOK https://www.facebook.com/business/help/279059996069252?id=2042840805783715 (last visited August 3, 2023).
[49] *Business Help Center: Add an ad account to a Meta Pixel in Meta Business Manager*, FACEBOOK https://www.facebook.com/business/help/622772416185967 (last visited August 3, 2023).

80. To add the Pixel to its website, the website operator can choose to add the Pixel code through (i) the "event setup tool" via "partner integration" or (ii) by manually adding the code to the website.

81. Manually adding base Pixel code to the website consists of a multi-step process, which includes: (i) creating the pixel; (ii) installing base code in the header of every webpage the Pixel is active, (iii) setting automatic advanced matching behavior, (iv) adding event code using an automated tool or manually,[50] (v) domain verification, and (vi) configuring web events.[51]

82. After following these steps, a website operator can start harvesting information using the Pixel.

83. A Pixel cannot be placed on a website by a third-party without being given access by the site's owner.

84. When a Facebook user logs onto Facebook, a "c_user" cookie – which contains a user's non-encrypted Facebook User ID number ("UID" or FID) – is automatically created and stored on the user's device for up to a year.[52]

85. A Facebook UID can be used, by anyone, to easily identify a Facebook user. Any person, even without in-depth technical expertise, can utilize the UID. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook UID to www.facebook.com (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular UID.

---

[50] Some users claim that automated tools for adding event code provide inconsistent results and recommend adding event code manually. *See* Ivan Mana, *How to Set Up & Install the Facebook Pixel (In 2022)*, YOUTUBE, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited August 3, 2023).

[51] *Business Help Center: How to set up and install a Meta Pixel*, FACEBOOK https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited August 3, 2023); *see* Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, YOUTUBE https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited August 3, 2023).

[52] *Privacy Center: Cookies Policy*, FACEBOOK https://www.facebook.com/policy/cookies/ (last visited August 3, 2023).

86. In addition to the c_user cookie, the Pixel also transmits personally identifying information connected with a PII User in the form of cookie identifiers, including IP address, browser fingerprints and device identifiers.

87. Browser-fingerprints is "information collected about a remote computing device for the purpose of identification."[53] Browser fingerprints include information such as "operating system, active plugins, time zone, language, screen resolution, and various other active settings."[54] A study in 2017 demonstrated that browser fingerprinting techniques can be used to successfully identify 99.24 percent of all users.[55]

b. The Pixel as a Tracking Method

88. The Pixel tracks user-activity on web pages by monitoring events which,[56] when triggered, causes the Pixel to automatically send data directly to Facebook.[57]

89. Examples of events utilized by websites are: (i) "microdata" tags (the "Microdata event"),[58] and (ii) visiting webpages with a Pixel installed (the "PageView event").[59] The Healthcare Defendant's Website utilized all three of these Pixel events.[60]

90. When a PageView event is triggered, a "HTTP Request" is sent to Facebook (through Facebook's URL www.facebook.com/tr/).[61] This confirms that the Pixel events sent data to Facebook.

---

[53] *What Is Browser Fingerprinting? How It Works And How To Stop It*, PIXELPRIVACY https://pixelprivacy.com/resources/browser-fingerprinting/ (last visited August 3, 2023).
[54] *What Is Browser Fingerprinting? How It Works And How To Stop It*, PIXELPRIVACY https://pixelprivacy.com/resources/browser-fingerprinting/ (last visited August 3, 2023).
[55] Yinzhi Cao, Song Li and Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, NDSS (Feb. 27, 2017) https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/ (last visited August 3, 2023).
[56] *Meta Business Help Center: About Meta Pixel*, FACEBOOK https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited August 3, 2023).
[57] *See generally Id.*
[58] *Facebook Microdata Installing Schema*, CAT HOWELL https://cathowell.com/facebook-microdata-what-it-is-how-to-set-it-up/ (last visited August 3, 2023).
[59] *Meta Business Help Center: Specifications for Meta Pixel standard events*, FACEBOOK https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited August 3, 2023).
[60] The presence of Pixel events, such as the Microdata and PageView events, can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See Business Help Center: About the Meta Pixel Helper*, FACEBOOK https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited August 3, 2023).
[61] *How We Built a Meta Pixel Inspector*, THE MARKUP https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (last visited August 3, 2023).

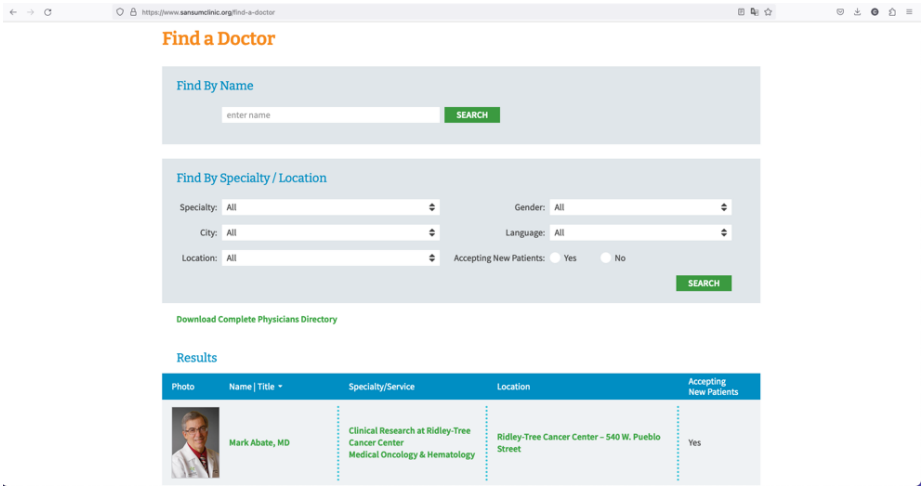
91. The HTTP Request includes a Request URL, embedded cookies such as the c_user cookie. It may also include information in its Payload, such as metadata tags.

92. A Request URL, in addition to a domain name and path, typically contains parameters. Parameters are values added to a URL to transmit data and direct a web server to provide additional context-sensitive services, as depicted below:

Figure 1 – Mozilla's diagram of a URL, including parameters[62]

93. PII Users experienced the detrimental consequences of Facebook's illicit gathering and dissemination of their PHI. Plaintiffs, as users of the Website, had their sensitive personal health information shared with Facebook, without their consent.

94. To demonstrate the Pixel's operation on the Website, when a PII User utilizes the Website to find a doctor, by clicking "find a doctor," they are subsequently prompted to enter information such as their gender and the specialty of the doctor they are looking for:



The Website's Find a Doctor Webpage

95. A PII User searching to find a doctor to treat a mental health condition, for example, is prompted to select "Psychiatry" as a "Specialty." These doctors are part of Healthcare Defendant's hospital network. The "Find a Doctor" page of the Website is used to solicit

[62] *What is a URL?*, MOZILLA https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited August 3, 2023).

prospective PII Users who are considering becoming patients of Healthcare Defendant for specific conditions.

96. When PII Users search to find a doctor through the Website, all their interactions with the Website are disclosed to Facebook, including what type of doctor they are looking for related to their specific health conditions, and the doctors they are ultimately considering. When a user clicks on a specific doctor based on their specialty or other specific features, that information is sent to Facebook along with the PII User's unique Facebook ID captured in the c_user cookie. In the case of the Website's "Find a Doctor" page, the PII User's PHI is shared through the *MicroData* Pixel event. The *MicroData* Pixel Event triggers whenever a webpage containing metadata tags established by Healthcare Defendant is loaded onto the user's browser.[63] This is depicted below in *Figure 1:*

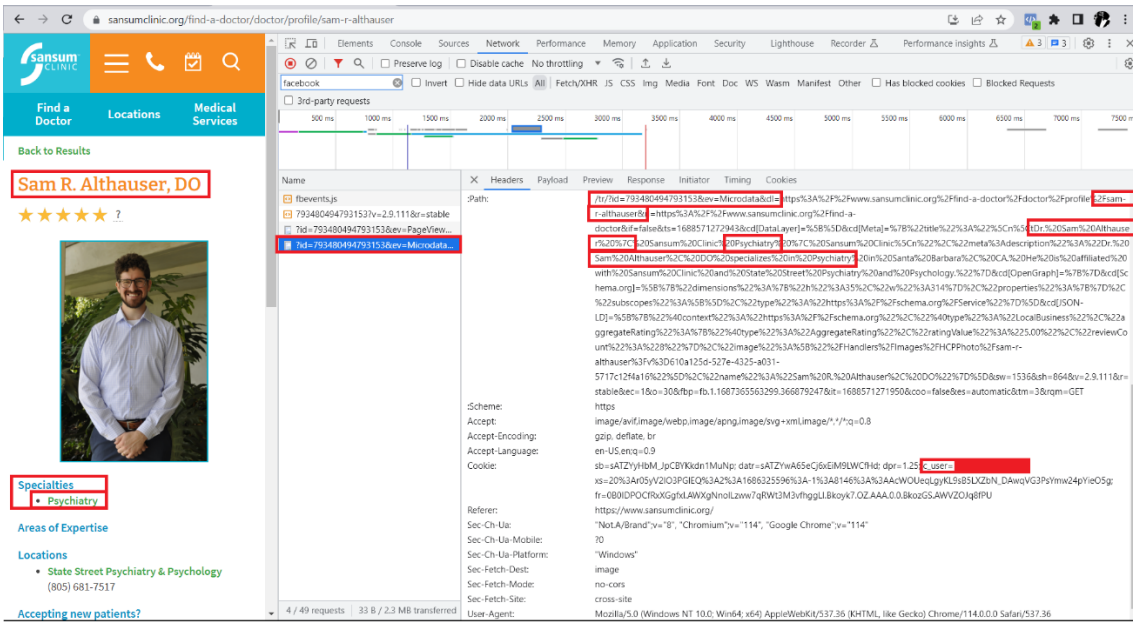


Figure 1, Screenshot of Data Transmission via Microdata Pixel Event when PII User uses the Find a Doctor Function on the Website

97. In addition to the information captured by the *MicroData* Pixel Event depicted above in *Figure 1,* the *PageView* Pixel Event captures information PII User searched for and

[63] *What are the Subscribedbuttonclick and MicroData events and can/should I disable this?*, FARMER'S RANDOM WEB/AD TECH PROBLEMS (Dec. 28, 2017) http://randomproblems.com/subscribedbuttonclick-microdata-events-can-disable-facebook-pixel-autoconfig-feature/ (last visited August 3, 2023).

transmits this information along with the PII User's Facebook ID to Facebook. This is depicted below in *Figure 2:*

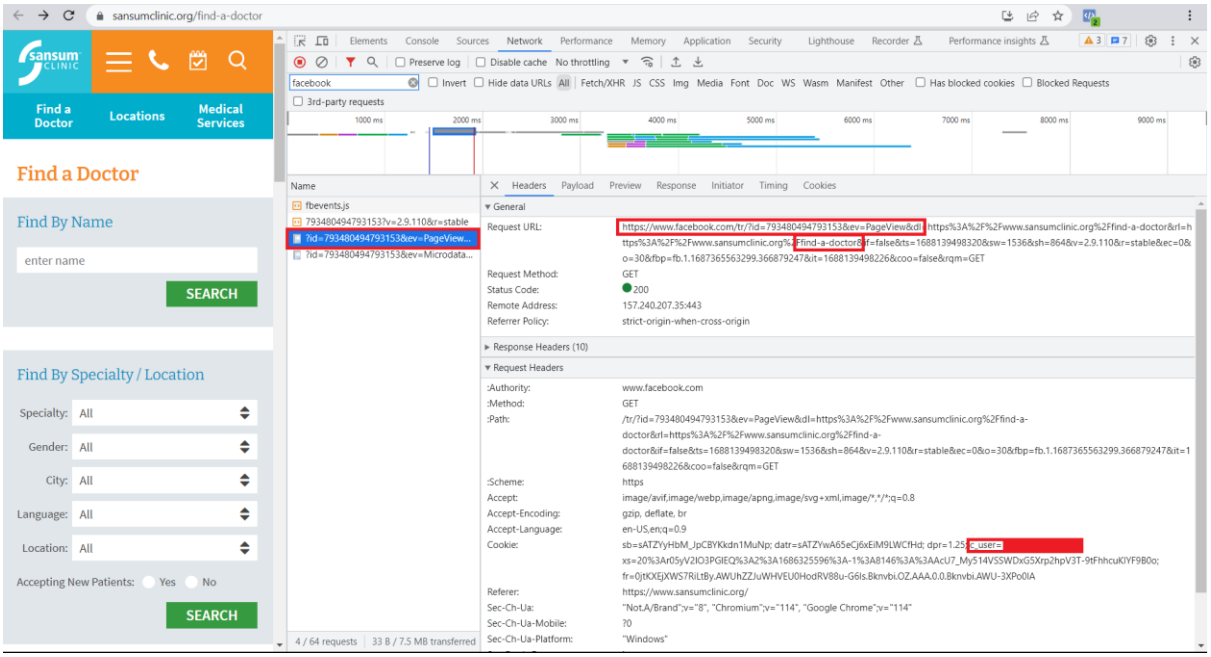


Figure 2, PageView Pixel Event captures URL and discloses it, and FID, to Facebook in a single transmission

98. The information disclosed to Facebook is typically censored for healthcare providers.[64] However, Healthcare Defendant discloses this information along with the PII User's unique Facebook ID, enabling Facebook to link the PII User's protected PHI with the user's unique FID, and then identify that specific PII User. The above representation of data transmission is consistent across all searches conducted on the Healthcare Defendant's Website.

99. In addition to transmitting a PII User's doctor search information, Healthcare Defendant also surreptitiously intercepts and relays PII User's search terms to Facebook.

100. The search function of the Website is used as a method to entice and maintain the Website visitors' interaction, including for prospective PII Users who are considering becoming patients of Healthcare Defendant for specific conditions.

101. Healthcare Defendant prompts PII Users to search for information related to their medical conditions (*i.e.*, "Cancer," "Diabetes," and "Pregnancy Care") on the Website.

[64] *Business Help Center: About Sensitive Health Information*, FACEBOOK https://www.facebook.com/business/help/361948878201809?id=188852726110565 ("If Meta's signals filtering mechanism detects Meta Business Tools data that it categorizes as potentially sensitive health-related data, the filtering mechanism is designed to prevent that data from being ingested . . . .") (last visited August 3, 2023).

Unbeknownst to PII Users, however, the Website's search function to find information on conditions, the Website's search function not only shares their PHI, but also shares their PII through the Pixel's transmission of the user's FID associated with that user's activity. In the case of the Website's search function, the search results pages on the Website contain *MicroData* tags, which result in the transmission of PII User's PHI and PII to Facebook, as shown below in *Figure 3:*

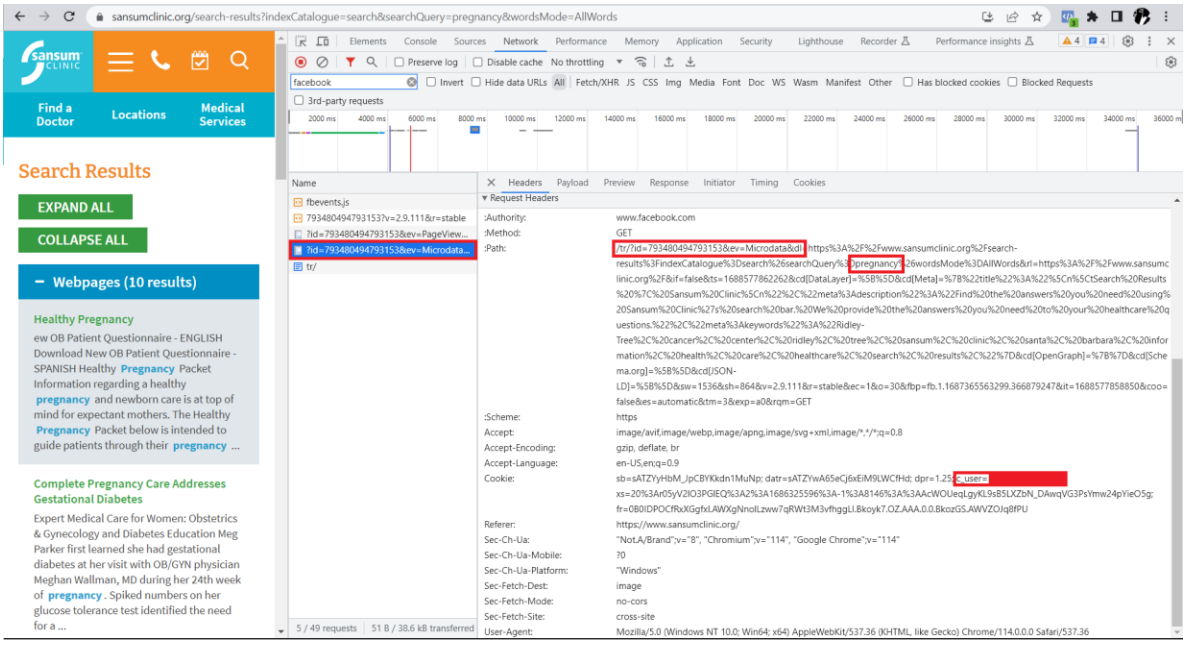


Figure 3, Screenshot of User's Search Results page on the Website, and Search Terms Associated with that User's Search being Disclosed by the Microdata Pixel Event

102. The search results additionally include links to services offered by Healthcare Defendant related to their PHI.

103. The data transmission represented in Figure 3 is consistent across all searches conducted through the Healthcare Defendant's Website.

104. As evident from the search results displayed in *Figure 3* above, the information a user searches on the Website can reveal extremely personal information related to that individual's PHI. By conducting a simple search for "Pregnancy" on the Website, the user tells Facebook that the PII User is likely pregnant or is looking for a doctor to help assess a pregnancy. This process results in Facebook obtaining knowledge that the PII User is potentially pregnant, with no input

from the PII User. Nothing on the Website indicates to PII Users that utilizing the Website's search function will reveal their PHI along with the exact content of their communications with the Website. This process is automatic, surreptitiously collecting and transmitting users PII and PHI to Facebook for advertising purposes. Upon clicking "Search" to search the Website for information related to their PHI, the Pixel Event is triggered, showing the Pixel's transmission of the PII User's PHI to Facebook.

105. The data disclosed by Healthcare Defendant includes prospective and actual patient information from other sections of the Website as well; *i.e.*, communications collected when a PII User searches for services or classes offered by Healthcare Defendant. As a result of this process, Facebook receives information from Healthcare Defendant including a full-string detailed URL, which includes the name of the website, the web pages the PII User viewed, the name of the doctor a PII User is considering, and search terms entered by the PII User. Additionally, Healthcare Defendant cause the transmission of PII User's cookie identifiers, including IP address, browser fingerprints and device identifiers.

106. By integrating the Website with code that results in the disclosure of PII User's PHI, Healthcare Defendant knowingly disclosed information that allowed Facebook and advertisers to link PII User's PHI to their identities and target them based on their personal health conditions. Healthcare Defendant purposefully shares their users' PHI with Facebook in order to financially benefit from the Pixel tool.

E. Plaintiffs and Class Members Do Not Provide Authorization to Defendants to Collect and Disclose their PHI

107. The Healthcare Defendant has not, and does not, seek nor obtain authorization from their PII Users, including Plaintiffs and the Class, to share the PII User's PHI with third parties, including Facebook.

108. Plaintiffs and the Class were unaware that Healthcare Defendant actively collects their sensitive PHI when visiting the Website, searching for doctors, and searching for information related to their health conditions on the Website. The presence of the Pixel is completely inconspicuous, as it is seamlessly integrated and hidden in the background of the Website's code.

109. When an individual creates a Facebook account, they enter into an agreement with Facebook by accepting and acknowledging the Terms, Data Policy, and Cookie Policy. This agreement is confirmed through a checkbox on the sign-up page. Both Facebook and its users are obligated to abide by these binding Terms, Data, and Cookie Policies.

110. Facebook Data Policy explicitly states that businesses utilizing the Pixel are obligated to possess legal rights to collect, use, and share user data before sharing any data with Facebook.[65]

111. Facebook does not verify whether the businesses utilizing the Pixel has indeed obtained the necessary consent.

112. Facebook relies on its business customers to police themselves. Businesses need only "represent and warrant" that they have adequately and prominently notified users about the collection, sharing, and usage of data through their Business Tools.

113. The Pixel can be accessed by any business or publisher regardless of the nature of their business. It is worth noting that the collection of sensitive medical information belonging to the Plaintiffs contradicts the other provisions outlined in Facebook's Data Privacy policy. Specifically, Facebook claims that each of its supposed "partners" is obligated to possess lawful rights to collect, use, and share user data before providing it to Meta. However, Healthcare Defendant does not have the legal authority to use or share the data of the Plaintiffs and the Class, as this information is protected under HIPPPA. HIPPA covers all electronically protected health information generated, received, maintained, or transmitted by a covered entity like Healthcare Defendant. The rule explicitly prohibits the use and disclosure of protected health information to Facebook for targeted advertising purposes, as stated in 45 C.F.R. § 164.502. In essence, Facebook contracts with healthcare providers, like Healthcare Defendant, but fails to ensure compliance with its own Terms and with state and federal law protecting sensitive health information.

[65] https://www.facebook.com/business/help/1057016521436966?id=188852726110565

F. Defendants Knew that Pixel Would Reveal Plaintiffs' PHI and Other Sensitive Medical Information, Including their Health Conditions

114. Healthcare Defendant knew or should have known that by utilizing the Pixel on the Website, they would disclose Plaintiffs' and Class Members' sensitive PHI to Facebook.

115. Due to the nature of how Pixel functions, which involves sending all user website interactions to Facebook, the Healthcare Defendant was advised that its users' sensitive data would be transmitted to Facebook when users engaged in any form of interaction on their websites, such as looking up information related to a health condition or assessing a health condition.

116. Facebook is aware that by allowing healthcare providers to implement its Facebook Pixel on to their websites, it facilitates the gathering of sensitive PHI belonging to the PII Users of those healthcare providers. Facebook knows that it receives this PHI and it uses this PHI to improve its advertising processes.

117. Facebook spokesman Dale Hogan said that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people through [its] Business Tools," and that their systems are "designed to filter out potentially sensitive data," those policies and procedures have not been enforced or have been completely ineffective.[66]

118. To that point, a complaint by the Federal Trade Commission filed in 2021, exhibited that Facebook received medical information through its Business Tools for years. The FTC concluded that Facebook had used that sensitive information for their own research and development purposes.

119. In or around February 2021, the New York State Department of Financial Services (NYSDFS) reached a similar determination. It found that Facebook had collected sensitive data, including medical information, in violations of its own policies. NYSDFS stated that simply "[m]erely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate fact is that Facebook does little to track whether . . . developers are violating this rule and takes no real action against developers that do." The NYSDFS stated that Facebook's "Facebook's

[66] Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022) https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story (last visited August 3, 2023).

efforts here [are] seriously lacking" and that "[u]ntil there are real ramifications for violating Facebook's policies, Facebook will not be able to effectively prohibit the sharing of sensitive user data with third-parties."

120. The Markup article also reported that its investigation into Facebook's "filtering" system revealed that Facebook failed to delete the most obvious forms of sexual health information, which included the URLs with information related to abortion, which stated "post-abortion" "i-think-im-pregnant" and "abortion-pill."

121. Additionally, documents leaked to the news organization *Vice* in 2021 exposed that Facebook's employees acknowledged or confirmed Facebook's inability to effectively manage the way its systems utilize data. A Facebook engineer working on the Ad and Business Product team stated that "We do not have adequate level of control and explain ability over how our systems use data, and thus we can't confidentially make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"

> A research director at UC Berkley in the Usable Security and Privacy Group has stated that Facebook just does not have the incentive to enforce its own privacy policies because "[t]hat costs them money to do. As long as they're not legally obligated to do so, why would they expend any resources to fix [it]?"[67]

122. Healthcare Defendant purposefully disclosed Plaintiffs' communications to Facebook to improve the effectiveness of their advertising and marketing or to place-third party ads on the Website.

123. Plaintiffs did not know of or consent to the dissemination of their communications with Healthcare Defendant to Facebook.

124. Facebook was not a party to the communications, as Plaintiffs did not know of their involvement in the communications, and Facebook used the intercepted communications for their benefit independent of any benefit to Healthcare Defendant.

[67] Grace Oldham and Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, REVEAL (June 15, 2022) https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ (last visited August 3, 2023).

G. Plaintiffs and Class Members possess a Reasonable Expectation of Privacy in their Sensitive Medical Information and Related Information

125. Plaintiffs and Class Members have a reasonable expectation of privacy in their PHI and sensitive medical information.

126. Specifically, PII User's health information is protected under federal law by HIPPA and California State law through the CMIA.

127. HIPAA establishes nationwide guidelines for protecting confidential health information. As one example, HIPPA imposes restrictions on the acceptable purposes for using health information and expressly prohibits disclosure without explicit authorization. C.F.R. § 164.502. Additionally, HIPAA mandates that entities subject to its provisions must implement suitable measures to safeguard such information. 45 C.F.R. § 164.530(c)(1).

128. This legal framework applies to healthcare providers; here, the Healthcare Defendant.

129. Pursuant to HIPPA's protections applicable to Healthcare Defendant, Plaintiffs and the Class Members had a reasonable expectation of privacy in their protected health information.

130. Studies investigating the gathering and release of individuals' sensitive medical data validate that the act of disclosing such information from millions of users without consent infringes upon established societal norms and expectations of privacy.[68]

131. Consumer surveys indicate that consumers are "most willing to share their health information when privacy protections are in place, with consent being the most important, followed by data deletion, regulatory oversight and data transparency."[69]

132. As an illustration, a recent survey conducted by Consumer Reports indicated that 92% of Americans hold the opinion that websites and internet companies should be obligated to seek consent before selling or sharing consumers' data. Similarly, the same percentage believe that these companies should be mandated to furnish consumers with a comprehensive inventory

---

[68] Jessica Hagen, *Survey: Privacy protections boost consumers' willingness to share health data*, MOBIHEALTH NEWS (Mar. 7, 21023) https://www.mobihealthnews.com/news/survey-privacy-protections-boost-consumers-willingness-share-health-data (last visited August 3, 2023).

[69] *Id.*

of the information collected about them.[70] Another study by *Pew Research Center* concluded that approximately 79% of Americans, are concerned about how data is collected about them by companies.[71]

133. User behavior conforms to these statistics: after the introduction of a new version of the iPhone operating software, which requests explicit and affirmative consent from users before permitting companies to track them, a substantial majority of users who were presented with the prompt opted not to share their data when – worldwide users (85%) and U.S. users (94%).[72]

134. Heightening the concern associated with the sharing of medical information is exasperated by the reality that advertisers place a high value on this type of information. Allowing advertisers to access women's sexual health information, for example, allows advertisers to obtain information on unborn children. An article addressing this concern stated: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[73] The article goes on to emphasize that:

> Children today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles.[74]

135. Privacy law experts have voiced their concern regarding the sharing of users' sensitive medical information with third parties. Dena Mendelsohn, the prior Senior Policy Counsel at Consumer Reports, and current Director of Health Policy and Data Governance at Elektra Labs, has explained that the dissemination of personal health information without one's

---

[70] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/ (last visited August 3, 2023).

[71] Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, PEW RESEARCH CENTER (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last visited August 3, 2023).

[72] Margaret Taylor, *How Apple screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook (last visited August 3, 2023).

[73] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER (Jan. 14, 2023) https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/ (last visited August 3, 2023).

[74] Id.

awareness could have significant consequences, such as impacting the ability to secure life insurance and influencing the cost of coverage.[75] Additionally, Mendelsohn stated that could lead to higher interest rates on loans and leave individuals more susceptible to workplace discrimination.[76]

136. Without their knowledge or consent, Defendants have surreptitiously collected and shared Plaintiffs' and Class Members' personal information and personal health information, through Pixel, in violation of their privacy interest.

H. The Economic Value of Plaintiffs' and Class Members' Personal Health Information

137. Facebook's business is built around collecting personal data. This is unsurprising given that the "world's most valuable resource is no longer oil, but data."[77] As stated in the *Economist*, personal data is "the oil of the digital era."[78]

138. There is a large economic market for consumers personal data within the tech industry, including the type of data collected from Plaintiffs and Class Members.

139. A *Financial Times* article published in 2013 reported that the data-broker industry has reaped tremendous profits from trading thousands of details regarding individual's "age, gender and location" information which are sold for about "$0.50 per 1,000 people."[79]

140. Similarly, *TechCrunch* has reported that "to obtain a list containing the names of individuals suffering from a particular disease," someone within the market would have to spend about "$0.30 per name."[80] That article explained further that the value of a single user's data (in the corporate acquisition context) can range from $15 to $40 per user.[81] The article notes that

---

[75] Donna Rosato, What Your Period Tracker App Knows About You, CONSUMER REPORTS (Jan. 28, 2020) https://www.consumerreports.org/health/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/ (last visited August 3, 2023).
[76] *Id.*
[77] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data (last visited August 3, 2023) (emphasis added).
[78] *Id.*
[79] Emily Steel, et al., *How much is your personal data worth?*, FINANCIAL TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz3myQiwm6u (last visited August 3, 2023).
[80] Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?*, TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited August 3, 2023).
[81] *Id.*

"Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[82]

141. An article published by the Washington Post in 2021 by the legal scholar Dina Srinivasan explained that consumers "should think of Facebook's cost as [their] data, and scrutinize the power it has to set its own price."[83] The value of this information is only increasing. Facebook's financial statements reveal that from 2013 to 2020, the value of the average American's data in the advertising context rose from $19 to $164 per year.[84]

142. In a paper published in 2013 by the Organization for Economic Cooperation and Development ("OECD"), the OECD measured the prices that were being demanded by companies for user information, similar to that at issue here, derived from "various online data warehouses."[85] The OECD found that, at that time, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[86]

143. Importantly, a 2021 report by Invisibly found that personal medical information is one of the most valuable pieces of information within the market for data. The report noted that "[i]t's worth acknowledging that because health care records often feature a more complete collection of the PII User's identity, background, and personal identifying information (PII), health care records have proven to be of particular value for data thieves. While a single social security number might go for $0.53, a complete health care record sells for $250 on average. For criminals, the more complete a dataset, the more potential value they can get out of it. As a result, health care breaches increased by 55% in 2020."[87]

---

[82] *Id.*
[83] Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/ (last visited August 3, 2023).
[84] *Id.*
[85] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD DIGITAL ECONOMY PAPERS, NO. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited August 3, 2023).
[86] Id.
[87] Id.

144. This article provided a complete breakdown of the average price per record type:

Record Type	Average Price
Health Care Record	$250.15
Payment Card Details	$5.40
Banking Records	$4.12
Access Credentials	$0.95
Social Security Number	$0.53
Credit Record	$0.31
Basic PII	$0.03

145. Individuals can even choose to monetize their own personal data if they choose to do so.

146. An article published by the Verge notes that Facebook has offered individuals money for their voice recordings,[88] and has also offered teens and adults up to $20 a month plus referral fees to install software allowing Facebook to collect data on how individuals us their smartphones.[89]

147. Additionally, various other companies and apps such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.[90]

I. Facebook's Long History of Privacy Violations

148. Facebook has maintained its core business model around monetizing user information since 2007 to the expense of its users. This is evident from a complaint filed by the

[88] Jay Peters, Facebook will now pay you for your voice recordings, THE VERGE (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognitionviewpoints-prounnciations-app

[89] Saheli Roy Choudhury and Ryan Browne, Facebook pays teens to install an app that could collect all kinds of data, CNBC (Jan. 29. 2019) https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html (last visited August 3, 2023).

[90] 28 Apps That Pay You For Data Collection: Earn a Passive Income, DOLLAR BREAK (July. 7, 2022), https://www.dollarbreak.com/apps-that-pay-you-for-data-collection/ (last visited August 3, 2023).

Federal Trade Commission ("FTC") in 2019 against Facebook which noted that ""substantially all of Facebook's $55.8 billion in 2018 revenues came from advertising."[91]

149. During its launch in 2007, Facebook introduced the "Facebook Beacon" without users being informed about the tracking of their online activities, and initially, there was no option for users to op-out. Following widespread criticism, Facebook Beacon was eventually discontinued.

150. Facebook reached another settlement with the FTC in November of 2011 related to their sharing of Facebook user information with advertisers. In addition, the settlement covered claims that Facebook had falsely asserted that third-party apps were only able to access data which they needed to operate, when in reality, the third-party apps could access nearly all of Facebook's users' personal data. The Chairman of the FTC, Jon Leibowtize, warned that "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users . . . Facebook's innovation does not have to come at the expense of consumer privacy."[92]

151. The 2011 FTC settlement resulted in a Consent Order which prohibited Facebook from misrepresenting the level of control consumer have over their privacy settlings, the necessary actions consumers need to take to exercise those controls, and the extent to which Facebook allows third-parties to access user information.[93]

152. Another Facebook privacy scandal arose in April of 2015 when a report showed that Facebook could not track how many developers were using previously downloaded Facebook user information.

153. In 2018, Meta faced scrutiny once more due to its failure to safeguard users' privacy. During congressional hearings, Facebook disclosed that a company named Cambridge Analytica potentially obtained the data of approximately 87 million users in relation to the 2016 presidential election. Consequently, the Federal Trade Commission (FTC) launched another

[91] Complaint For Civil Penalties, Injunction, And Other Relief, *United States v. Facebook, Inc.*, Case No. 19-cv-2184-TJK (D.C. July 24, 2019), ECF No. 1.
[92] *Id.*
[93] Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012)

investigation in 2019 to examine Facebook data collection methods and privacy policies. The investigation concluded with a historic settlement of five billion dollars.

154. Thereafter, an investigation uncovered that Facebook had breached users' privacy consent by granting more than 150 companies access to users' information.[94] As a result, certain companies even had the ability to read users' private messages. Paradoxically, this arrangement assisted Meta in attracting a larger user base.

155. In June 2020, despite assuring users that app developers would not be able to access their data if they had been inactive for 90 days, Facebook disclosed that it had still allowed third-party developers to retrieve such data.[95] As a consequence of their failure to safeguard user data, thousands of developers were able to view information about inactive Facebook users, provided that those users were connected on Facebook with an active user.

156. Finally, in June 2022, a settlement was reached between Facebook and the U.S. Department of Justice regarding allegations that the company enabled landlords to engage in discriminatory practices when advertising housing through Meta's ad targeting tool called "Lookalike Audiences." It was alleged that this tool facilitated targeting users based on sensitive characteristics such as race, gender, religion, and more. As a result of the settlement, Meta agreed to discontinue the use of this discriminatory targeting tool.

157. In spite of Facebook's long history of grievous privacy violations, it continues to collect highly sensitive medical information without consent and in disregard to the privacy rights of its users, including Plaintiffs and Class Members.

CLASS ACTION ALLEGATIONS

158. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

Nationwide Class: All natural persons in the United States whose PHI was collected through Facebook's Pixel through the Website.

---

[94] Elizabeth Schulze, *Facebook let tons of companies get info about you, including Amazon, Netflix, and Microsoft*, CNBC (Dec. 19, 2018), https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html (last visited August 3, 2023).

[95] Kurt Wagner And Bloomberg, *Facebook admits another blunder with user data*, FORTUNE (July 1, 2020), https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/ (last visited August 3, 2023).

California Subclass: All natural persons residing in California whose PHI was collected through Facebook's Pixel through the Website.

159. Specifically excluded from the Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

160. Plaintiffs reserve the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

161. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

162. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Class. However, given the popularity of Defendant's Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

163. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Class, was a prospective PII User and user of the Website, and used, a Website to assess a health condition and search for information related to a health condition, and had their PHI and PII collected and disclosed by Healthcare Defendant.

164. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

165. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered

by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

166. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

a. Whether Healthcare Defendant collected Plaintiffs' and Class Members' PHI;

b. Whether Healthcare Defendant unlawfully disclosed and continue to disclose the PHI of PII Users in violation of the CIPA, CMIA and the Federal Wiretap Act;

c. Whether Healthcare Defendant's disclosures were committed knowingly, willfully or intentionally;

d. Whether Healthcare Defendant's disclosures of Plaintiffs' and Class Members' PHI was without consent or authorization;

e. Whether Facebook collected Plaintiffs' and Class Members' PHI;

f. Whether Facebook unlawfully intercepts the PHI of PII Users in violation of the CIPA, CMIA and the Federal Wiretap Act;

g. Whether Facebook's interception was committed knowingly, willfully, or intentionally; and

h. Whether Defendants' material omissions regarding the practices alleged herein constitute an unfair and/or deceptive practice under the Arizona Consumer Fraud Act.

167. Information concerning Healthcare Defendant's data sharing practices, including with respect to the identities of prospective PII Users, is available from Healthcare Defendant's or third-party records.

168. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

169. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

170. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

171. Given that Defendants' conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
FIRST CLAIM FOR RELIEF
Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Nationwide Class)
Against Facebook

172. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

173. Plaintiffs assert claims for intrusion upon seclusion and so pleads that: Facebook intentionally intruded into a place, conversation, or matter as to which Plaintiffs and the Nationwide Class had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

174. Facebook intentionally intruded upon Plaintiffs' and Nationwide Class Members' seclusion through its interception and collection of communications transmitted between PII Users, including Plaintiffs and Class Members, and the Healthcare Defendant, including sensitive medical information, in the form of PHI, without obtaining consent or authorization for such disclosure from Plaintiffs and the Nationwide Class.

175. Plaintiffs and Nationwide Class Members maintained a reasonable expectation of privacy when they provided their sensitive medical information to Healthcare Defendant through

their communications with Healthcare Defendant on the Website. Personal medical information is widely recognized by society as sensitive information that cannot be shared with third parties without the explicit consent. For example, public polling shows that, "[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent."[96]

176. Plaintiffs' and Nationwide Class Members' reasonable expectation of privacy is supported by HIPPA's recognition that medical data is sensitive information that must be protected from unauthorized disclosure.

177. Plaintiffs and Nationwide Class Members maintained a reasonable expectation of privacy believing that Facebook would not disclose their communications with Healthcare Defendant as a medical provider, because Facebook affirmatively promised users that it would require its business partners to only share information with Facebook that could be lawfully shared.

178. Plaintiffs and Nationwide Class Members possessed a reasonable expectation of privacy based on the belief that Facebook would abide by state criminal laws, such as the California Invasion of Privacy Act ("CIPA"). CIPA prohibits Facebook from intercepting communications between patients, such as Plaintiffs and the Class, and their healthcare providers without the consent of all parties involved in the communication (both the PII User and the healthcare provider).

179. As explained above, Facebook's actions constitute a serious invasion of privacy that was an egregious breach of social norms, such that the breach was highly offensive to a reasonable person because:

a. the invasion of privacy occurred in a highly sensitive setting – PII Users' communications with their healthcare provider;

b. Facebook had no legitimate objective or motive in invading Plaintiffs' and Nationwide Class Members' privacy;

[96] *Poll: Huge majorities wants control over health info,* HEALTHCARE FINANCE https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info (last visited August 3, 2023).

c. Facebook violated multiple laws by invading Plaintiffs' and Nationwide Class Members' privacy, including the California Invasion of Privacy Act and the Wiretap Act;

d. Facebook deprived Plaintiffs and Nationwide Class Members of the ability to control dissemination of their personal medical information; and

e. Facebook's actions are also unacceptable as a matter of public policy because they undermine the relationship between patients and their healthcare providers.

180. Facebook's interception and collection of Plaintiffs' and Nationwide Class Members' communications with Healthcare Defendant is also so extensive as to constitute oppression, malice, or fraud.

181. As a direct and proximate result of this infringement upon their privacy, Plaintiffs and Nationwide Class Members sustained harm and experienced various damages. In light of these injuries, Plaintiffs and Nationwide Class Members are pursuing suitable remedies, such as compensatory damages, restitution, disgorgement, punitive damages, and any other relief that the Court deems appropriate and fair.

COUNT II
Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Nationwide Class)
Against Healthcare Defendant

182. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

183. Plaintiffs and Nationwide Class Members maintained a reasonable expectation of privacy in their communications with Healthcare Defendant via its Website. Medical data is widely recognized by society as sensitive information that cannot be shared with third parties without the PII Users' explicit consent. For example, public polling shows that, "[n]inety-seven

percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent."[97]

184. Plaintiffs' and Nationwide Class Members' reasonable expectation of privacy is supported by HIPPA's recognition that patient medical data is sensitive information that must be protected from unauthorized disclosure.

185. Plaintiffs and Nationwide Class Members maintained a reasonable expectation of privacy believing that Healthcare Defendant would not their personal communications with Healthcare Defendant, as a medical provider, because Healthcare Defendant were under a duty to not share such information with Facebook unless they had explicit authorization to do so.

186. Plaintiffs and Nationwide Class Members possessed a reasonable expectation of privacy based on the belief that Healthcare Defendant would abide by state criminal laws, such as the CIPA. CIPA prohibits Facebook from intercepting communications between patients, such as Plaintiffs and the Nationwide Class, and their healthcare providers without the consent of all parties involved in the communication (both the PII User and the healthcare provider). Through its placement of Pixel on the Website, Healthcare Defendant's enabled this interception and resulting intrusion upon Plaintiffs' and Nationwide Class Member's privacy.

187. As explained above, Healthcare Defendant's actions constitute a serious invasion of privacy that was egregious breach of social norms, such that the breach was highly offensive to a reasonable person because:

a. the invasion of privacy occurred in a highly sensitive setting – PII Users' communications with their healthcare provider;

b. Healthcare Defendant had no legitimate objective or motive in invading Plaintiffs' and Class Members' privacy in such a manner;

c. Healthcare Defendant violated multiple laws by invading Plaintiffs' and Nationwide Class Members' privacy, including the CIPA and the Wiretap Act;

[97] *Poll: Huge majorities wants control over health info,* HEALTHCARE FINANCE https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info (last visited August 3, 2023).

d. Healthcare Defendant deprived Plaintiffs and Nationwide Class Members of the ability to control dissemination of their personal medical information; and

e. Healthcare Defendant's actions are also unacceptable as a matter of public policy because they undermine the relationship between patients and their healthcare providers.

188. Healthcare Defendant's transmission of Plaintiffs' and Nationwide Class Members' communications with Healthcare Defendant is also so extensive as to constitute oppression, malice, or fraud.

189. As a direct and proximate result of this infringement upon their privacy, Plaintiffs and Nationwide Class Members sustained harm and experienced various damages. In light of this injury, Plaintiffs and Nationwide Class Members are pursuing suitable remedies, such as compensatory damages, restitution, disgorgement, punitive damages, and any other relief that the Court deems appropriate and fair.

COUNT III
Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On Behalf of Plaintiffs and the California Subclass)
Against Facebook

190. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

191. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

192. California voters added the word "and privacy" to the California Constitution when they passed Proposition 11 in 1972. Proposition 11 is also known as the "Privacy Initiative" or "Right to Privacy Initiative."

193. In support to Proposition 11, voters stated that: The right of privacy is the right to be left alone … It prevents government and business and business interests from collecting and

stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

194. Both Plaintiffs and the California Subclass Members have a legally protected interest in their sensitive medical data and other information they send and receive to their healthcare providers through the Website, which Facebook violates through its intercepting of such communications. Plaintiffs' and California Subclass Members' protected interests come from various statutes and common law, including:

a. HIPPA;

b. The Wiretap Act;

c. The California Invasion of Privacy Act;

d. The California Constitution, which protects the rights of privacy, and includes the "the ability to control circulation of our personal information;" and

e. Facebook's contracts, which "require each of these partners to have lawful rights to … share your data before providing any data to" Facebook.

195. The privacy rights of Plaintiffs and California Subclass Members were invaded through the interception and collection of the data transmitted between PII Users (including Plaintiffs and Class Members) and their healthcare providers, here Healthcare Defendant, which included their sensitive medical information, without first obtaining authorization or consent from Plaintiffs and California Subclass Members.

196. Plaintiffs and California Subclass Members had a reasonable expectation of privacy when communicating with Healthcare Defendant online and thereby providing their PHI to their healthcare provider. It is widely recognized that sensitive medical data cannot be shared with third parties without a patient's consent. This is evident from public polls showing that "[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology

systems should not be allowed to share or sell their sensitive health information without consent."[98]

197. This reasonable expectation of privacy in their PHI harbored by Plaintiffs and California Subclass Members is supported by HIPPA's recognition that medical data is sensitive information.

198. Plaintiffs' and California Subclass Members' reasonable expectation of privacy is further supported by Facebook's affirmative promise that it would require its partners to only share data with Facebook that could be lawfully shared.

199. Plaintiffs and California Subclass Members maintained a reasonable expectation of privacy in their PHI supported further by their understanding that Facebook would not violate state criminal laws, such as the CIPA, in intercepting their communications with healthcare providers without the consent of both parties to the communications.

200. As detailed above, Facebook's acts in intercepting these Plaintiffs' and California Subclass Member's communications constitute a serious violation of social norms, and as such their breach is highly offensive to a reasonable person for the following reasons:

a. There was no legitimate objective for or motive or Facebook in invading Plaintiffs' and Class Member's privacy rights;

b. Facebook did not allow Plaintiffs and Class Members the ability to control the dissemination of their personal medical information;

c. Multiple laws, including the Wiretap Act and California Invasion of Privacy Act, were violated due to Facebook's invasion of Plaintiffs' and Class Members' privacy;

d. The context of the communication between PII Users and their healthcare providers is highly sensitive; and

[98] *Poll: Huge majorities wants control over health info,* HEALTHCARE FINANCE https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info (last visited August 3, 2023).

e. Public policy also dictates that Facebook's actions undermine the relationship between Plaintiffs, California Subclass, and healthcare providers.

201. Plaintiffs and California Subclass Members were injured and suffered damages as a direct and proximate result of Facebook's actions in invading their privacy rights. Thus, Plaintiffs and California Subclass Members seek relief for those injuries including compensatory damages, restitution, disgorgement, punitive damages, and any other relief that the Court may deem just and proper.

COUNT IV

Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On Behalf of Plaintiffs and the California Subclass)

Against Healthcare Defendant

202. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

203. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

204. California voters added the word "and privacy" to the California Constitution when they passed Proposition 11 in 1972. Proposition 11 is also known as the "Privacy Initiative" or "Right to Privacy Initiative."

205. In support to Proposition 11, voters stated that: The right of privacy is the right to be left alone … It prevents government and business and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

206. Both Plaintiffs and the California Subclass Members have a legally protected interest in their sensitive medical data and other information they send and receive to their

healthcare providers through the Website, which Facebook violates through its intercepting of such communications. Plaintiffs' and California Subclass Members' protected interests come from various statutes and common law, including:

a. HIPPA;

b. The Wiretap Act;

c. The California Invasion of Privacy Act;

d. The California Constitution, which protects the rights of privacy, and includes the "the ability to control circulation of our personal information;" and

e. Facebook's contracts, which "require each of these partners to have lawful rights to … share your data before providing any data to" Facebook.

207. The privacy rights of Plaintiffs and California Subclass Members were invaded through the interception and collection of the data transmitted between PII Users (including Plaintiffs and Class Members) and their healthcare providers, here Healthcare Defendant, which included their sensitive medical information, without first obtaining authorization or consent from Plaintiffs and California Subclass Members.

208. Plaintiffs and California Subclass Members had a reasonable expectation of privacy when communicating with Healthcare Defendant online and thereby providing their PHI to their healthcare provider. It is widely recognized that sensitive medical data cannot be shared with third parties without a patient's consent. This is evident from public polls showing that "[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent."[99]

209. This reasonable expectation of privacy in their PHI harbored by Plaintiffs and California Subclass Members is supported by HIPPA's recognition that medical data is sensitive information.

[99] *Poll: Huge majorities wants control over health info,* HEALTHCARE FINANCE https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info (last visited August 3, 2023).

210. Plaintiffs' and California Subclass Members' reasonable expectation of privacy is further supported by Facebook's affirmative promise that it would require its partners to only share data with Facebook that could be lawfully shared.

211. Plaintiffs and California Subclass Members maintained a reasonable expectation of privacy in their PHI supported further by their understanding that Facebook would not violate state criminal laws, such as the CIPA, in intercepting their communications with healthcare providers without the consent of both parties to the communications.

212. As detailed above, Healthcare Defendant's acts in intercepting Plaintiffs' and California Subclass Member's communications constitute a serious violation of social norms, and as such their breach is highly offensive to a reasonable person for the following reasons:

213. There was no legitimate objective for or motive for Healthcare Defendant in invading Plaintiffs' and California Subclass Member's privacy rights;

a. Healthcare Defendant did not allow Plaintiffs and California Subclass Members the ability to control the dissemination of their personal medical information;

b. Multiple laws, including the Wiretap Act and California Invasion of Privacy Act, were violated due to Facebook's invasion of Plaintiffs' and California Subclass Members' privacy;

c. The context of the communication between Plaintiffs, California Subclass, and their healthcare providers is highly sensitive; and

d. Public policy also dictates that Healthcare Defendant' actions undermine the relationship between Plaintiffs, California Subclass, and healthcare providers.

214. Plaintiffs and California Subclass Members were injured and suffered damages as a direct and proximate result of Facebook's actions in invading their privacy rights. Thus, Plaintiffs and California Subclass Members seek relief for those injuries including compensatory damages, restitution, disgorgement, punitive damages, and any other relief that the Court may deem just and proper.

COUNT V
Violation of California Confidentiality of Medical Information Act
Civil Code Section 56.06 ("CMIA")
(On Behalf of Plaintiffs and the California Subclass)
Against Healthcare Defendant

215. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

216. Healthcare Defendant is a provider of health care under Cal. Civ. Code. Section 56.06, subdivision (a) and (b), as they offer software to consumers that are designed to maintain medical information, do manage such medical information, and allow users to manage their medical information or for the treatment, management, or diagnosis of a medical condition.

217. As a provider of health care, Healthcare Defendant is bound by subdivision (b) of the CMIA (Confidentiality of Medical Information Act) and are obligated to uphold the same standards of confidentiality as required of a provider of health care with respect to the medical information they maintain on behalf of PII users, including Plaintiffs and the California Subclass.

218. By failing to maintain the confidentiality of users' medical information, in the form of their PHI, and disclosing that information to third parties, without the consent of Plaintiffs and California Subclass, Healthcare Defendant has violated Civil Code section 56.06.

219. Plaintiffs' and California Subclass Members' PHI was disclosed to third parties, including Facebook, who are in the business of selling advertisements based on that data they collect regarding individuals. In this case, the PHI disclosed to those third parties, including Facebook, was that of Plaintiffs and California Subclass Members, based on their communications with Healthcare Defendant's Website.

220. Healthcare Defendant's disclosure of Plaintiffs' and California Subclass Members' PHI was done knowingly and willfully, and without the consent of Plaintiffs and California Subclass. Importantly, in violation of Civil Code section 56.06 subdivisions (b) and (c), Healthcare Defendant's disclosures were made for financial gain, including to utilize the data to market and advertise the services they provide, or to allow others to do the same. Healthcare Defendant was aware that implementation of Pixel would result in the capture of Plaintiffs' and California Subclass Members' PHI inputted while using their Website, yet decided to implement

it despite this knowledge. This demonstrates Healthcare Defendant's knowledge and willful disclosure of Plaintiffs' and California Subclass Members' PHI.

221. At a minimum, Healthcare Defendant has negligently disclosed the personal medical information of Plaintiffs and California Subclass Members to Facebook in violation of Civil Code section 56.06 subdivisions (b) and (c).

222. As such, Plaintiffs and California Subclass Members seek redress in the form of: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to 56.36; (c) and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VI
Aiding and Abetting Violation of California CMIA
Civil Code Section 56.06, 56.101, 56.10
(On Behalf of Plaintiffs and California Subclass)
Against Facebook

223. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

224. Healthcare Defendant's disclosure of Plaintiffs' and California Subclass Member's sensitive medical information as alleged herein violates several provisions of the CMIA.

225. Moreover, Facebook acted intentionally or, alternatively, with knowledge that Healthcare Defendant's disclosure of Plaintiffs' and California Subclass Members' sensitive medical information was a violation of the CMIA as evident from Facebook's contracting with Healthcare Defendant to receive and utilize Plaintiffs' and Class Members' sensitive medical information.

226. Facebook actively encouraged and supported Healthcare Defendant in its violation of the CMIA by providing Healthcare Defendant with Pixel, which once implemented, it knew would cause their Website to share and disclose Plaintiffs' and California Subclass Members' sensitive medical information.

227. Facebook's agreement with Healthcare Defendant, and their receipt of Plaintiffs' and California Subclass Members' sensitive personal medical information is a substantial factor causing Fakebook's violations of the CMIA.

228. Without Pixel provided to Healthcare Defendant by Facebook, Healthcare Defendant would not have shared Plaintiffs' and California Subclass Members' sensitive medical information as described herein.

229. As outlined herein, Facebook has aided and abetted Healthcare Defendant's CMIA violations and therefore is jointly liable, along with Healthcare Defendant, for the relief sought by Plaintiffs and the California Subclass.

COUNT VII
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200 et. seq.
(On Behalf of the Plaintiffs and the California Subclass)
Against Facebook

230. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

231. As Facebook has violated the California common law, California Constitution, and other statutes and common law privacy claims, Facebook's business acts and practices are "unlawful" under the Unfair Competition Law Cal. Bus. & Prof. Code §§ 17200 et. seq. ("UCL").

232. Under the UCL, Facebook's business acts and practices are "unfair." As explained herein, California public policy strongly favors protecting consumer's privacy interest, including the protection of consumers' personal data. Facebook's surreptitious collection, disclosure, and misuse of Plaintiffs' and California Subclass Members' sensitive medical information violated California public policy. Facebook's conduct has repeatedly violated the polices of all the statues referenced herein.

233. Facebook's business actions constitute "fraudulent" business acts and practices within the meaning of the UCL. Plaintiffs and California Subclass Members had no knowledge of the large collection of their sensitive medical information disclosed to Facebook, Facebook has thus acted without consumer's consent or knowledge.

234. Facebook has expressly indicated to Facebook users that it would receive only data from its business "partners," and that those partners would be "require[d]" to have lawful rights to collect, use and share [users'] data before providing any data to [Facebook]." The PHI collected by Healthcare Defendant and disclosed to Facebook does not meet this requirement as it is

protected by the Health Insurance Portability and Accountability Act of 1996's Privacy Rule, which makes unlawful the disclosure of this information without authorization from Plaintiffs and California Subclass Members. See 45 C.F.R. § 160.103. As such, Facebook's actions were fraudulent because it represented to Plaintiffs and California Subclass Members that their PHI would not be collected, but it collected that information anyway.

235. The business actions and practices of Facebook were likely to, and ultimately did, deceive members of the public including Plaintiffs and California Subclass Members into believing this data was private.

236. As explained above, Facebook's violations were willfully deceptive, unfair, and unconscionable.

237. Plaintiffs and California Subclass Members would not have used Facebook had they known that their sensitive medical information was collected, associated with their Facebook, Instagram, and other media accounts provided by Facebook, and then used for Facebook's own benefit.

238. Plaintiffs and California Subclass Members have a protected property interest in their sensitive medical information at issue here. Through its surreptitious collection and disclosure of Plaintiffs' and California Subclass Member's PHI, Healthcare Defendant have taken property from Plaintiffs and California Subclass Members without providing just compensation.

239. As a result of Facebook's conduct in violation of the UCL, Plaintiffs and the California Subclass Members have lost money and property. As described above, sensitive health data of consumers, of the kind collected and used by Facebook objectively has value. Various companies are willing, and do, pay for health data, such as the sensitive medical data collected by Facebook here. As one example, Pfizer buys approximately $12 million worth of health data from various sources per year.[100]

240. Through its collection and use of Plaintiffs' and California Subclass Members' sensitive health data, Facebook has taken money or property from them without compensation.

[100] Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, SCIENTIFIC AMERICAN (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-yourmedical-records/ (last visited August 3, 2023).

241. Plaintiffs and California Subclass Members thus seeks restitution and compensatory damages for Facebook's violations of the UCL.

COUNT VIII
Violation of the Federal Wiretap Act, U.S.C. § 2510, et. seq.
(On Behalf of Plaintiffs and the Nationwide Class)
Against Facebook

242. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

243. Plaintiffs bring this claim individually and on behalf of the members of the proposed class against Facebook and Healthcare Defendant.

244. Codified under 18 U.S.C. U.S.C. §§ 2510 et seq., the Federal Wiretap Act (the "Wiretap Act") prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

245. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

246. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

247. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

248. The Wiretap Act defines "person as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

249. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

250. Facebook is a person under the Wiretap Act.

251. Pixel constitutes a "device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

252. The confidential communications between Plaintiffs and the Nationwide Class and Healthcare Defendant's Website, in the form of their PHI were intercepted by Facebook utilizing Pixel, and such communications were "electronic communications" under 18 U.S.C. § 2510(12).

253. The Wiretap Act is applicable to both the sending and receipt of communications.

254. Plaintiffs and the Nationwide Class had a reasonable expectation of privacy in their electronic communications with the Healthcare Defendant's Website in the form of their PHI. Interception of Plaintiffs' and Nationwide Class Members' communications with the Healthcare Defendant's Website occurs in the regular course of using the Healthcare Defendant's Website to search for information related to health conditions and assess health conditions. Moreover, Facebook is not a party to these communications.

255. Facebook violated the Wiretap Act by utilizing the communications that they intercepted to create target audiences and lookalike audiences. 18 U.S.C. § 2511(1)(c).

256. The interception and use Plaintiffs' and Nationwide Class Members' communications with their health care provider, Healthcare Defendant was intentional and knowing as indicated by: (a) Facebook's promotion of its Facebook Pixel to healthcare providers, such as Healthcare Defendant, for use on their websites; (b) Facebook's promotion that utilizing Pixel on the healthcare providers websites would allow them to create custom audiences; and (c) Facebook's failure to prevent health care providers from transmitting personal medical data to Facebook using Pixel.

257. Facebook's interception of these communications occurred contemporaneously with Plaintiffs and Class Members sending and receiving those communications.

258. The intercepted communications, in the form of PHI, between Plaintiffs, the Nationwide Class Members, and the Website constitute the "contents" of the communications for purposes of the Wiretap Act.

259. Facebook did not receive consent from Plaintiffs or the Nationwide Class before it intercepted, disclosed, and used their sensitive PHI with Healthcare Defendant. Indeed, such

consent could not have been given as neither Facebook nor Healthcare Defendant ever sought any form of consent from Plaintiffs or the Nationwide Class to intercept, record, and disclose their private communications with the Healthcare Defendant's Website.

260. As detailed above, Facebook's unauthorized interception, disclosure and use of Plaintiffs' and the Nationwide Class Members' PHI was only possible through Facebook's knowing, willful, or intentional placement of Pixel on the Website. 18 U.S. Code § 2511(1)(a).

261. Plaintiffs and the Nationwide Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications Facebook in violation of 18 U.S.C. § 2520. As such, Plaintiffs and the Nationwide Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Nationwide Class and any profits made by Facebook as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) appropriate equitable or declaratory relief; (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT IX
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, et seq. ("CIPA")
(On Behalf of Plaintiffs and the California Assessment Subclass)
Against Healthcare Defendant and Facebook

262. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

263. Plaintiffs bring this count on behalf of themselves and all members of the California Assessment Subclass.

264. CIPA provides that a person is liable to another where, "by means of any machine, instrument, contrivance, or in any other manner," committed any of the following: (i) intentionally tapped, or made any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, cable, or instrument of any internal telephonic communication system; or (ii) willfully and without consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or

communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or (iii) uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or (iv) aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit or cause to be done any of the acts or things mentioned above in this section. Cal. Penal Code Section 631(a).

265. "Courts agree . . . that CIPA § 631(a) applies to communications conducted over the internet." *Yoon v. Lululemon United States*, 549 F. Supp. 3d 1073, 1080 (C.D. Cal. July 15, 2021).

266. The Ninth Circuit has confirmed that one of the purposes of wiretapping statutes is to "prevent the acquisition of the contents of a message by an unauthorized third-party . . . ." *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020). In dealing specifically with CIPA, the California Supreme court has similarly concluded that the objective of CIPA is to protect a person's communications "from a situation where the other person on the other end of the line permits an outsider" to monitor the communication. *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985); see *Smith v. LoanMe*, 11 Cal. 5th 183, 200 (2021).

267. California Penal Code § 637.2 provides a private right of action for violations of CIPA so that "[a] person who has been injured by a violation of [CIPA] may bring an action against the person who committed the violation…"

268. As Healthcare Defendant conducts business in California, California law governs its relationship with the PII Users from California.

269. Healthcare Defendant's Website, including Pixel placed upon it, is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

270. Within the relevant time period, Plaintiffs and members of the California Assessment Class used the health assessment tool on the Website to communicate personal health information to Healthcare Defendant, with the expectation of receiving results provided by Healthcare Defendant.

271. Within the relevant time period, Facebook, without the consent of all parties to the communication, or in any unauthorized manner, willfully read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and the putative California Assessment Class, contemporaneous with the communications transit through or passing over any wire, line, or cable or with the communications sending from or being received at any place within California.

272. Within the relevant time period, Facebook willfully learned or attempted to learn the contents of communications between Plaintiffs, California Assessment Class members, and their healthcare providers, through the Healthcare Defendant's Website.

273. Within the relevant time period, Healthcare Defendant aided, agreed with, conspired with, and employed Facebook to implement Pixel and to accomplish the wrongful conduct at issue here.

274. These violations of §§ 631 and 632 constitute an invasion of privacy sufficient to confer Article III standing.

275. Plaintiffs and the California Assessment Class did not authorize or consent to the tracking, interception, and collection of any of their electronic communications, in the form of their PHI.

COUNT X
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)
Against Healthcare Defendant

276. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 158 through 171 as though fully set forth herein.

277. Plaintiffs and the Nationwide Class entered into an implied contract with Healthcare Defendant when they provided their PHI to Healthcare Defendant in exchange for services, pursuant to which Healthcare Defendant agreed to safeguard their PHI and not disclose such information without consent.

278. Plaintiffs and Nationwide Class Members accepted Healthcare Defendant's offer and provided their PHI to Healthcare Defendant.

279. In the absence of an implied contract to not disclose their PHI without consent, Plaintiffs and the Nationwide Class Members would not have entrusted their PHI to Healthcare Defendant.

280. Healthcare Defendant breached its implied contracts by disclosing Plaintiffs' and Nationwide Class Members' PHI to Facebook.

281. As a direct and proximate result of Healthcare Defendant's breach of its implied contracts, Plaintiffs and the Nationwide Class have been injured as alleged herein. Had Plaintiffs and Nationwide Class Members known that their private PHI would be disclosed to Facebook, Plaintiffs and Nationwide Class Members would not have used Facebook's services, or would have been substantially less for those services.

282. As such, Plaintiffs and Nationwide Class Members are entitled to nominal, compensatory, and consequential damages as a result of Facebook's breach of implied contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of their respective classes and their counsel as Class Counsel;

(b) For an order declaring that the Defendants' conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to, requiring Defendants to immediately (i) remove the Pixel from the Website or (ii) add, and obtain, the appropriate consent from PII Users;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) An award of statutory damages or penalties to the extent available;

(g) For pre-judgment interest on all amounts awarded;

(h) For an order of restitution and all other forms of monetary relief;

(i) An award of all reasonable attorneys' fees and costs; and

(j) Such other and further relief as the Court deems necessary and appropriate.

DATE: August 10, 2023

Respectfully submitted,

LAW OFFICES OF TODD M. FRIEDMAN

By: */s/ Adrian R. Bacon*

Adrian R. Bacon, Esq.
21031 Ventura Blvd, Suite 340
Woodland Hills, CA 91364
Tel.: (323) 306-4234
Facsimile: (866) 633-0228
Email: abacon@toddflaw.com

Mark S. Reich*
LEVI & KORSINSKY, LLP
55 Broadway, 4th Floor, Suite 427
New York, NY 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com

Attorneys for Plaintiffs

**pro hac vice* forthcoming